



Universidad de Murcia

Facultad de Informática

PROPUESTA DE UNA INFRAESTRUCTURA DE CLAVE
PÚBLICA Y SU EXTENSIÓN MEDIANTE UN SISTEMA DE
GESTIÓN DISTRIBUIDA DE CREDENCIALES BASADO EN
DELEGACIÓN Y ROLES

TESIS DOCTORAL

Presentada por:
Óscar Cánovas Reverte

Supervisada por:
Dr. Antonio Fernando Gómez Skarmeta
Departamento de Ingeniería de
la Información y las Comunicaciones

Murcia, Octubre de 2002



Universidad de Murcia

D. Antonio Fernando Gómez Skarmeta, Profesor Titular de Universidad del Área de Ingeniería Telemática en el Departamento de Ingeniería de la Información y las Comunicaciones de la Universidad de Murcia, AUTORIZA:

La presentación de la Tesis Doctoral titulada “Propuesta de una infraestructura de clave pública y su extensión mediante un sistema de gestión distribuida de credenciales basado en delegación y roles”, realizada por D. Óscar Cánovas Reverte, bajo su inmediata dirección y supervisión, y presentada para la obtención del grado de Doctor por la Universidad de Murcia.

En Murcia, a 28 de Octubre de 2002
D. Antonio Fernando Gómez Skarmeta

Resumen

La criptografía de clave pública ha sido ampliamente reconocida como una tecnología fundamental sobre la cual pueden construirse varios servicios básicos de seguridad. Los principales esfuerzos de los últimos quince años se han concentrado en el problema de asignar de forma segura nombres a claves. De hecho, la comunidad científica ha ido progresivamente adoptando el uso de sistemas basados en el estándar X.509 con el fin de proporcionar servicios de seguridad a los sistemas distribuidos, los cuales dependen de la existencia de un método seguro y fiable de gestión de las claves públicas denominado infraestructura de clave pública (PKI, Public Key Infrastructure).

Las PKIs deben proporcionar mecanismos para gestionar todas las operaciones relacionadas con el ciclo de vida de los certificados digitales, es decir, su generación, distribución, validación y revocación. Sin embargo, la mayoría de los diseños e implementaciones actuales no proporcionan un tratamiento completo a todas estas cuestiones, especialmente a las relacionadas con la revocación, la validación o el cumplimiento de las políticas de certificación. La PKI que se presenta como una de las contribuciones de esta tesis subsana esta falta de soporte mediante la provisión de varios mecanismos diseñados para poder realizar una gestión completa de los certificados X.509.

Por otro lado, durante los últimos años, la criptografía de clave pública ha sido propuesta también como una herramienta para solucionar los problemas relacionados con la autorización y el control de acceso, es decir, para determinar qué están autorizadas a realizar las entidades de un sistema distribuido. De hecho, son varias las especificaciones existentes que proponen mecanismos capaces de ligar información de seguridad a claves públicas. Más concretamente, dichas especificaciones han desarrollado notaciones para asignar autorizaciones y para propagar dichas autorizaciones entre varias claves.

Sin embargo, tales propuestas no especifican cómo debe realizarse la gestión del ciclo de vida de los certificados de autorización. Si bien ciertos enfoques dependientes de la aplicación pueden dar resultado en entornos reducidos, su uso en escenarios complejos puede sacar a relucir varios problemas relacionados con su escalabilidad e interoperabilidad, lo cual hace necesario plantear un sistema que sea capaz de llevar a cabo dicha gestión de forma estructurada y distribuida. Por tanto, una de las principales contribuciones de esta tesis es la definición de una infraestructura de autorización. Dicha infraestructura está compuesta de un sistema distribuido de gestión de credenciales basado en delegación y roles, un marco para el intercambio seguro de información de autorización y una metodología de definición de políticas de autorización.

En consecuencia, tanto la PKI como la infraestructura de autorización constituyen un sistema global para la gestión distribuida de certificados digitales. Con el fin de demostrar su aplicabilidad como middleware de seguridad, se presenta también como parte de este trabajo la integración de dicho sistema en dos escenarios de aplicación distintos.

Abstract

Public key cryptography is widely recognized as being a fundamental technology on which several essential security services can be built. Much security discussion over the past 15 years has concentrated on the problem of assigning names to keys. Related to this, the Internet community is agreeing on the use of systems based on the X.509 standard in order to provide basic security services to distributed systems. These services need a practical and reliable method of publishing the public keys, called a Public Key Infrastructure (PKI).

PKIs must provide the mechanisms to manage all the operations related to the lifecycle of digital certificates, i.e., generation, distribution, validation, and revocation. However, most of the current designs and implementations of PKIs do not provide a wide coverage to all these issues, especially to those topics related to revocation, validation, or policy enforcement. The PKI presented as a contribution of this thesis overcomes this lack of support providing several mechanisms that have been designed to perform a complete management of X.509 certificates.

On the other hand, in recent years, public key cryptography has been also proposed as a tool for solving the problems related to authorization and access control, that is, for determining what the identities should be allowed to do in a distributed environment. Several specifications propose mechanisms for capturing security-relevant information and binding that information to public keys. They have also developed languages for assigning authorizations and for delegating those authorizations from one key to another.

Nevertheless, these proposals do not explain how the lifecycle of authorization certificates is performed. Although simple and not distributed approaches can constitute a good alternative for small scenarios, some problems derived from scalability or interoperability might arise in more complex environments. A structured and distributed system must be provided to manage the generation or revocation of those certificates. Therefore, one of the main contributions of this thesis is the definition of an authorization infrastructure. That infrastructure consists of a distributed credential management system based on delegation and role membership, a framework for secure exchange of authorization-related information, and a methodology for the definition of authorization policies.

The PKI and the authorization infrastructure constitute a global system for distributed management of identity and authorization certificates. In order to demonstrate their feasibility and their suitability as a security middleware, two different application environments making use of their mechanisms are presented.

Agradecimientos

Supongo que gran parte de lo que es mi vida actual está condicionada por el hecho de que mi padre quisiera comprarle un ordenador personal a un niño de 8 años que pasó gran parte de su infancia trasteando a 4 MHz (y eso que no me dejaba usarlo mucho porque decía que me ponía nervioso). Por tanto, el primer agradecimiento es para él y para mi madre, por haberme dado todo lo que estaba en sus manos para poder dedicarme a lo que me gusta y ganarme la vida con ello. También a mi hermana Fani, por haber prestado siempre tanta atención a lo que le cuenta su hermano (aunque no siempre me entienda) y por hacerme ver las cosas de otro color.

Por supuesto, nada habría sido lo mismo sin el constante apoyo y cariño de Noemí, quien ha visto como esta tesis nos robaba demasiadas horas y, no contenta con eso, tuvo incluso la paciencia de revisar el estilo de este documento (eliminando así innovadoras aportaciones al castellano que yo había propuesto reiteradamente).

Al grupo de investigación ANTS, especialmente a las personas con las que he tenido la oportunidad de colaborar en los proyectos de seguridad (Gabi, Félix, Rafa, Antonio y Gregorio). La posibilidad de haber analizado, debatido, defendido y cuestionado con ellos muchas de las ideas aquí presentes ha enriquecido sin duda el resultado final (y si no, siempre nos queda la posibilidad de aceptar aquella oferta que nos hicieron para formar parte de un circo).

A los compañeros de DITEC, por haber sabido lograr este ambiente tan cálido con el cual es mucho más agradable trabajar. En especial a Pepe, al cual le debo tantas cosas (por ejemplo, la sección 2.4.2 ;-)) y del que he aprendido tanto que necesitaría un apéndice D para poder contarlo todo.

Por último, gracias a Antonio por haber confiado en mi y haberme dado la oportunidad de trabajar a su lado.

Índice General

1	Introducción y objetivos	1
1.1	La seguridad como cuestión transversal	1
1.2	Evolución de la certificación digital	4
1.2.1	El papel de la criptografía	5
1.2.2	Certificación de la identidad	7
1.2.3	Certificación de los privilegios	9
1.3	Objetivos y aportaciones propias	10
1.4	Desarrollo de la Tesis	12
2	Infraestructuras de clave pública	15
2.1	Estándares de certificación digital de identidad	15
2.1.1	Modelos de confianza	16
	Modelo basado en autoridades de certificación específicas	16
	Telaraña de confianza (web of trust)	18
2.1.2	Adecuación a entornos de aplicación e implantación	18
2.2	El estándar X.509	19
2.2.1	Directorio X.500	20
2.2.2	Formato de los certificados X.509v3	21
2.3	Ciclo de vida de un certificado digital	23
2.3.1	Gestión de claves	24
2.3.2	Emisión de certificados	25
2.3.3	Distribución de certificados	26
2.3.4	Renovación de certificados	26
2.3.5	Revocación de certificados	27
2.3.6	Políticas y prácticas de certificación	27
2.4	Recomendaciones PKIX para el desarrollo de PKIs	28
2.4.1	Arquitectura de una PKI	29
2.4.2	Protocolos de gestión	30
	Certificate Management Protocol (CMP)	30
	Certificate Management over CMS (CMC)	31
2.4.3	Protocolos operacionales	31
	Validación de certificados	32
	Sellado de tiempo	33

2.5	Entornos de PKI	34
2.5.1	Desarrollos nacionales e internacionales	34
	PEM (Privacy Enhanced Mail)	34
	Secure Electronic Transaction (SET)	35
	Identrus	36
	EuroPKI	37
	Proyecto CERES	38
2.5.2	Desarrollos previos realizados en la Universidad de Murcia	38
3	Gestión de certificados X.509 y nuevos servicios	41
3.1	Objetivos a cumplir por la PKI desarrollada en el marco del Proyecto PISCIS	41
3.2	Diseño general de la PKI	42
3.2.1	Elementos participantes	43
	Entidades básicas	43
	Entidades de valor añadido	44
3.2.2	Relación entre los elementos	45
3.3	Operaciones básicas ofrecidas por la PKI	47
3.3.1	Certificación	47
	Creación de solicitudes en las autoridades de registro	48
	Creación de solicitudes usando el navegador	48
	Procesamiento de solicitudes de entidades software	48
3.3.2	Renovación	48
	Renovación basada en las autoridades de registro	49
	Renovación mediante conexión autenticada	49
3.3.3	Revocación	49
3.4	Una propuesta de política de seguridad para PKI	50
3.4.1	Motivación	50
3.4.2	Ciclo de vida de una política de PKI	51
3.4.3	Estructura de una política de PKI	52
	Elementos de política	52
3.4.4	Cumplimiento de las políticas	54
3.5	Propuestas de valor añadido para PKIs	54
3.5.1	Servicio de autorrevocaciones	55
	Revocación mediante conexión segura autenticada	56
	Revocación mediante autenticación en dos fases	57
3.5.2	Servicio de refirmado de certificados	58
	Diseño del sistema	60
	Dinámica del sistema	62
	Comparativa entre OCSP y la técnica de refirmado	65
	Comentarios finales	67
3.6	Conclusiones	67

4	Autorización basada en certificados	69
4.1	Carencias de la certificación de identidad	69
4.1.1	Respecto al control de acceso y la autorización	70
4.1.2	Respecto al anonimato	72
4.1.3	Respecto a la delegación de privilegios	73
4.1.4	Conclusiones	74
4.2	Modelos de control de acceso	74
4.2.1	Mandatory Access Control (MAC)	75
4.2.2	Discretionary Access Control (DAC)	75
4.2.3	Role Based Access Control (RBAC)	76
4.2.4	Control de acceso distribuido basado en delegación	78
4.3	Especificaciones de certificados de credencial	80
4.3.1	PolicyMaker	81
	Arquitectura del sistema	82
	Lenguaje de autorización	82
	Semántica de las consultas	83
	Firmas digitales y lenguaje de programación de los filtros	83
	Escenarios de uso	83
4.3.2	KeyNote	84
	Sintaxis de las aserciones	85
	Semántica de evaluación de las consultas	86
	Escenarios de uso	86
	Conclusiones	87
4.3.3	PMI (Privilege Management Infrastructure)	87
	Certificados de atributo X.509	88
	Delegación	90
	Modelos de PMI	91
	Escenarios de uso	91
	Conclusiones	92
4.3.4	SPKI/SDSI	93
	Terminología	93
	Nombres SDSI	94
	Certificados SPKI de identidad	95
	Certificados SPKI de autorización y de atributo	95
	Validación en SPKI	96
	Listas de control de acceso (ACL) y secuencias	97
	Cálculo de autorizaciones	97
	Cálculo de la cadena de certificación	99
	Escenarios de uso	99
	Conclusiones	100
4.3.5	Otros esquemas basados en XML	100
4.3.6	Conclusiones	101
4.4	Análisis del control de acceso basado en delegación	101

4.4.1	Estructuras de gestión	102
	Gestión de permisos	102
	Cadenas de delegación	103
	Control de la delegación	104
4.4.2	Autoridad y posesión de permisos	105
4.4.3	Anonimato	105
	Claves temporales	106
	Reducción y reductores confiables	107
4.4.4	Distribución y recuperación de certificados	107
	El problema de la <i>pertenencia oculta</i>	108
	El problema del <i>permiso oculto</i>	108
	Propuestas para el descubrimiento de certificados	109
4.4.5	Revocación	110
4.4.6	Soporte para la delegación en las especificaciones analizadas sobre certificados de credencial	111
4.5	Planteamiento de las soluciones proporcionadas	113
5	Infraestructura de autorización	115
5.1	Visión general del sistema	115
5.2	Marco de intercambio de información de autorización	118
5.2.1	Análisis de las propuestas actuales	119
	Enfoques alternativos	121
5.2.2	Objetivos generales del marco	122
5.2.3	Arquitectura del marco	123
	Session Management	124
	Request Management	124
	Authorization Results Management	125
	Error Management	126
	Data Stream Management	126
	Transport Convergence	126
5.2.4	El protocolo AMBAR como implementación del marco	127
	Notación empleada	127
	Módulo SM	128
	Módulo TC	130
	Módulos RM, ARM y DSM	130
5.2.5	Análisis de seguridad del protocolo	132
	Análisis del módulo TC	133
	Análisis de los módulos RM y ARM	133
	Análisis del módulo SM	134
5.2.6	Ventajas de AMBAR	134
5.3	Sistema de Gestión Distribuida de Credenciales	135
5.3.1	Motivación	136
	Uso de autoridades de autorización	136

6.2	Implementación del marco AMBAR	173
6.2.1	Integración de la arquitectura CDSA	174
6.2.2	Esquema de funcionamiento del protocolo	175
6.2.3	Interfaz de programación (API)	176
	AMBARContext	176
	AMBARClientSession	178
	AMBARServerDaemon	180
	AMBARServerSession	180
6.3	Implementación de DCMS	181
6.3.1	Visión general	182
6.3.2	Aplicación generadora de tags	182
6.3.3	Aplicación de asignación de privilegios	183
6.3.4	Aplicación de gestión de identificadores	184
6.3.5	Aplicación generadora de políticas	185
6.3.6	Aplicación de las autoridades	186
	Configuración de las propiedades de la autoridad	187
	Configuración de los parámetros AMBAR	187
	Especificación de las políticas	188
	Operaciones en modo desconectado	188
	Operaciones en línea	188
6.3.7	Aplicación de los solicitantes	189
	Gestión de claves temporales	190
	Configuración de autoridades	190
	Gestión de solicitudes	191
6.3.8	Conclusiones	192
6.4	Integración en un entorno de control de acceso físico	192
6.4.1	Propuesta centralizada	194
6.4.2	Propuesta descentralizada	195
	Motivación	195
	Diseño de la propuesta	196
6.4.3	Implementación de la propuesta distribuida	197
6.4.4	Aplicación de la metodología e integración con DCMS	198
	Escenario a gestionar	198
	Aplicación de los procedimientos de nivel 0	198
	Aplicación de los procedimientos del bloque AMS	200
	Aplicación de los procedimientos del bloque NMS	201
6.4.5	Conclusiones obtenidas	202
6.5	Integración en un entorno de suscripción electrónica	203
6.5.1	El protocolo SPEED	204
	Visión general	204
	Participantes	205
	Modelo de compra	205
6.5.2	Integración de la PKI	207

6.5.3	Implementación de la suscripción electrónica mediante certificados de credencial	207
	Solicitud de suscripción	208
	Presentación de justificantes	208
6.5.4	Conclusiones obtenidas	209
6.6	Evaluación de la infraestructura de autorización	209
6.6.1	Entorno de evaluación	210
6.6.2	Evaluación de la fase de negociación	210
6.6.3	Evaluación de la fase de solicitud y respuesta	211
6.6.4	Evaluación de la tramitación de solicitudes con DCMS	213
6.6.5	Conclusiones obtenidas a partir de la evaluación	214
6.7	Conclusiones	214
7	Conclusiones y líneas futuras	217
7.1	Conclusiones	217
7.2	Líneas futuras	221
A	Definición de las políticas de PKI	239
A.1	Estructura general de la política	239
A.2	Reglas de la política	240
B	Estructuras de datos del protocolo AMBAR	243
B.1	Transport Convergence	243
B.2	Error Management	244
B.3	Authorization Results Management	245
B.4	Request Management	246
B.5	Data Stream Management	247
B.6	Session Management	248
B.7	Valores criptográficos	251
B.7.1	Valores relacionados con el mensaje ActivateCrypto	251
B.7.2	Valores relacionados con el mensaje InitSession	252
B.7.3	Derivación de claves simétricas a partir del MasterSecret	252
C	Elementos de información de DCMS	253
C.1	Naming Management System	253
C.1.1	Solicitudes NMS	253
C.1.2	Políticas de nombramiento	254
C.2	Authorization Management System	254
C.2.1	Solicitudes AMS	254
C.2.2	Políticas de autorización	255
C.3	Reduction Management System	255
C.3.1	Solicitudes RMS	255
C.3.2	Políticas de reducción	255

Índice de Figuras

2.1	Modelo de confianza jerárquico	17
2.2	Modelo de certificación cruzada	17
2.3	Modelo de autoridad de certificación puente	18
2.4	Árbol de directorio X.500	21
2.5	Certificado X.509v3	22
2.6	Entidades de una PKI	29
2.7	Infraestructura PEM	35
2.8	Infraestructura SET	36
3.1	Colaboración entre las entidades de la PKI	45
3.2	Alternativas del proceso de certificación	47
3.3	Ejemplo de cumplimiento de la política	54
3.4	Autorrevocación mediante conexión autenticada	56
3.5	Autorrevocación en dos fases	58
3.6	Validación del certificado a refirmar	62
3.7	Obtención del certificado refirmado	64
3.8	Comparativa entre OCSP y refirmado	66
4.1	Relación entre elementos RBAC	77
4.2	Certificado de delegación	79
4.3	Cadena de delegación	80
4.4	Consulta PolicyMaker	82
4.5	Credenciales PolicyMaker	82
4.6	Aserciones KeyNote	85
4.7	Certificado de atributo X.509	89
4.8	Certificado SPKI de identidad	95
4.9	Certificados SPKI de autorización y atributo	96
4.10	Lista de control de acceso SPKI	97
4.11	Reducción de autorizaciones SPKI	98
5.1	Visión general del sistema	116
5.2	Enfoque común de control de acceso basado en certificados	120
5.3	Control de acceso basado en AMBAR	122
5.4	Arquitectura AMBAR	123

5.5	Ejemplo de optimización de solicitud de acceso	126
5.6	Gestión de flujos	132
5.7	Elementos de un entorno de control de acceso basado en delegación y roles	137
5.8	Estructura general de DCMS	140
5.9	Entidades de NMS	141
5.10	Solicitudes NMS	143
5.11	Políticas NMS	144
5.12	Entidades de RMS	151
5.13	Solicitudes RMS	152
5.14	Política de reducción	153
5.15	Comunicación AMBAR entre punto de acceso y autoridad	153
5.16	Metodología de definición de estructuras de gestión	155
5.17	Objetivo global del bloque de procedimientos AMS	161
5.18	Objetivo global del bloque de procedimientos NMS	163
6.1	Arquitectura CDSA	170
6.2	Integración de AMBAR con CDSA	174
6.3	Secuencia de estados de AMBAR	175
6.4	Clases de la API de AMBAR	177
6.5	Conjunto de aplicaciones DCMS	182
6.6	Aplicación de asignación de privilegios	183
6.7	Aplicación de gestión de identificadores	185
6.8	Aplicación generadora de políticas	186
6.9	Reducción de certificados en modo desconectado	189
6.10	Monitorización de las conexiones de la autoridad	190
6.11	Creación de solicitudes	191
6.12	Visión general de la propuesta centralizada	195
6.13	Arquitectura del sistema de control de acceso descentralizado	197
6.14	Roles de la jerarquía	198
6.15	Delegación de los controladores mediante ACLs	200
6.16	S-expresiones de la autoridad AA-Facultad	201
6.17	Modelo de compra de SPEED	206
6.18	Modelo de suscripción electrónica	208
6.19	Evaluación de la fase de negociación	211
6.20	Tiempo de acceso en función del número de credenciales	212
6.21	Tiempo de acceso en función del tamaño del recurso	212
6.22	Tiempo de tramitación de solicitudes	214